

Name : Vaibhav Soni

Enrolment No. : IU2141230287

Branch : CSE – A

Sem : 7

Subject : Cyber Security

Lab – 2

Aim : Port Scanning using NMAP.

Input :

`nmap -sV scanme.nmap.org`

Output :

```

(vaibhav3010@kali)-[~]
$ nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 22:03 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
1723/tcp  filtered pptp
5060/tcp  filtered sip
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.04 seconds
  
```

- The command ``nmap -sV scanme.nmap.org`` performs a service version detection scan on the domain ``scanme.nmap.org``. This command is used to scan the target ``scanme.nmap.org`` to identify open ports and determine the version of the services running on those ports. This helps in understanding the software and versions in use, which can be useful for security assessments and network inventory.

Input :

`nmap -sA scanme.nmap.org`

Output :

```

(vaibhav3010@kali)-[~]
$ sudo nmap -sA scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 22:18 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.068s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 22.90 seconds
  
```

- The command `nmap -sA scanme.nmap.org` performs an aggressive scan to determine firewall rules, detect service versions, and assess the operating system of the target `scanme.nmap.org`. It provides detailed information about the target's network defenses and services.

Input :

nmap -sS scanme.nmap.org

Output :

```
(vaibhav3010@kali)-[~]
└─$ sudo nmap -sS scanme.nmap.org
[sudo] password for vaibhav3010:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 22:16 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 983 closed tcp ports (reset), 1 closed tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
1074/tcp   filtered warmspotMgmt
1175/tcp   filtered dossier
1723/tcp   filtered pptp
5060/tcp   filtered sip
6692/tcp   filtered unknown
7443/tcp   filtered oracleas-https
8022/tcp   filtered oa-system
8300/tcp   filtered tmi
9929/tcp   open  nping-echo
13783/tcp  filtered netbackup
19315/tcp  filtered keyshadow
31337/tcp  open  Elite
54045/tcp  filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 90.33 seconds
```

- The command `nmap -sS scanme.nmap.org` performs a TCP SYN scan on the target `scanme.nmap.org`. It checks for open ports by sending SYN packets and analyzing the responses, providing a quick and stealthy method to identify active services on the target.

Input :

`nmap -sO scanme.nmap.org`

Output :

```
(vaibhav3010@kali)~$ sudo nmap -sO scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 22:20 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 254 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1         open  icmp
17        open  udp
Nmap done: 1 IP address (1 host up) scanned in 42.52 seconds
```

- The command ``nmap -sO scanme.nmap.org`` performs an IP protocol scan on the target ``scanme.nmap.org``. It identifies which IP protocols (such as ICMP, TCP, UDP) are supported by the target, helping to understand the network services and communication methods in use.